

Eye on RFID security

Designers can use this set of criteria when specifying RFID tags and readers for more information and security-intensive applications.

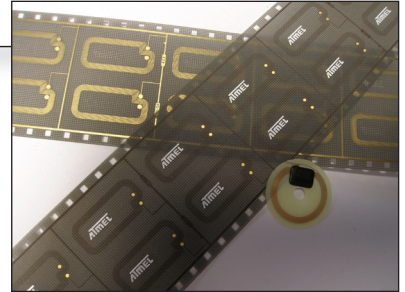
By Jean Pierre Benhammou and Martin Payne

RFID is rapidly gaining acceptance as a means of tracking products through the supply chain, in access control, and in more traditional applications such as ticketing. RFID systems typically consist of single-chip RFID tags with a radio, memory and controller, and an RFID reader that decodes the data on the tag and then takes an appropriate action (e.g., unlocking a door). RFID tags are labels that are similar to barcodes except that they electronically store product information. The newest RFID tags also offer the ability to update that information as a product travels through the supply chain, as well as security features.

RFID tags are used to track everything from household pets and livestock to high-end electronics. They automate toll collections on bridges and toll roads, and they restrict access to sensitive areas. Most recently, they have made inroads into more security-sensitive areas such as pharmaceuticals, contactless payment, cargo security and e-passports.

These information- and security-intensive applications mandate that new criteria must be used when specifying

Figure 1. Atmel offers a range of RFID tags with 64-bit read-only up to 64 kbit protected read/write memory, and 4 to 16 memory zones



RFID tags and readers. Such criteria include the memory available on the tag, the robustness of its encryption algorithms, and the number and security of different information “zones” on the tag. Let’s take a closer look.

The supply chain

RFID tags need to support more elaborate track and trace schemes. Consider pharmaceuticals. The number of counterfeit pharmaceuticals reported to the U.S. Food and Drug Administration (FDA) has grown tenfold in the last five years. In the worst-case scenario, a counterfeit drug could jeopardize a patient’s life. The stamps that manufacturers put on pills can be duplicated in such a way that a fake pill looks identical to the real pill from the manufacturer. Although barcodes on the packaging can provide extra information and an extra measure of security, they can be easily scanned or photocopied, and applied to the packaging of the counterfeit product. It is estimated that, worldwide, 10% of prescription drugs are counterfeit—costing tens of thousands of lives each year.

To stem the tide of counterfeit drugs, Florida mandated that as of July 1, 2006, prescription drugs must have a paper pedigree that includes the name of the drug, dosage form, strength, manufacturer, quantity by lot number, corresponding invoice/shipping/transfer document number, transaction dates, name and address of each owner, name and address of each recipient, certification of authentication, contact information for each wholesaler, a signature or oath that the pedigree is accurate and complete, and the manufacturer’s tracking number, when available. California will require an electronic pedigree by Jan. 1, 2009. Other states will follow.

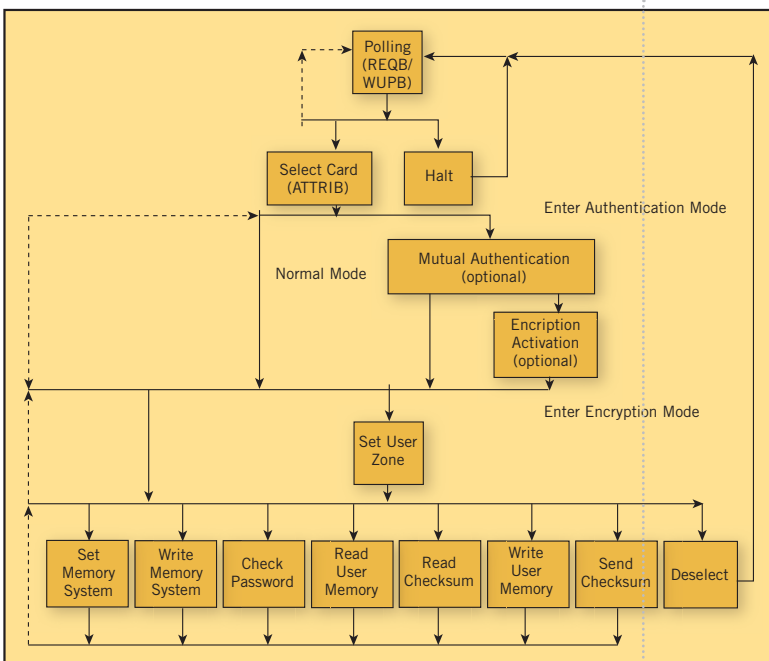


Figure 2. A block diagram of the typical security process for an RFID system.

Keeping track of this much information is a tall order for many RFID tags on the market because it requires a substantial amount of on-chip memory that must be able to be configured into multiple secure zones. For example, the manufacturer's ID, date of manufacture and product specifics should be able to be read by everyone, but should only be able to be written by the manufacturer. The retailer's ID needs to be writable by the shipping distributor but also capable of being updated by authorized personal at the retailer's location.

This type of data- and security-intensive application can require as much as 64 kbits of on-chip EEPROM and as many as 16 different user zones (Figure 1). Designers should take care that the tag vendor offers sufficient memory densities and user-configurability for the application at hand. The vast majority of tags have 2 kbits or less of memory and are usually limited to just two zones. While this memory density is generous if you are tracking an animal, it is not nearly enough to keep track of the information of every recipient in a complex supply chain.

RFID security

Security is the stepchild of RFID systems. Unfortunately, that security—typically provided by the vendors of the tags and tag readers—has been woefully inadequate (Figure 2). The majority of RFID tags on the market use outdated encryption algorithms with 48-bit keys that can be cracked in a few hours using a notebook PC. Consider that in the pharmaceutical example cited above, cracking the password would enable a drug counterfeiter to label fake drugs in exactly the same way as the manufacturer.

There have been improvements, however. Some RFID vendors are providing tags and readers that provide advanced crypto algorithms with 64-bit keys. Moving from 48- to 64-bits is not just a 50% improvement. Since the number of combinations and permutations of the factorial of the key length, a 64-bit algorithm is 64,000 times stronger than a 48 bit algorithm ($64 - 48 = 16/2$ 16ths = 64,000) and, therefore, more difficult to crack than a 48-bit key.

Given the catastrophic consequences that can result from the low level of security in most RFID tags, designers should select tags that offer robust, secure, crypto algorithms, with key length of at least 64 bits.

Tag readers

System developers should keep in mind that the security of the RFID tag is only as good as the tag reader used to read it. In other words, the 64-bit crypto algorithm on an advanced RFID tag is useless unless the tag reader or host supports it. As with the RFID tag, the majority of tag readers on the market support only minimal security, with outdated encryption algorithms and key lengths that make them much too easy to crack (Figure 3).

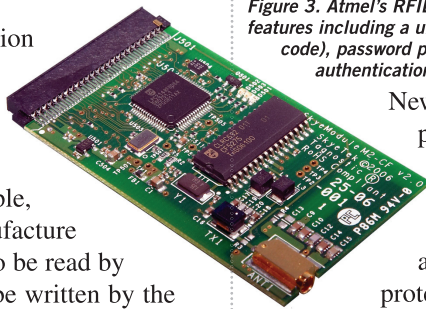


Figure 3. Atmel's RFID tags and readers flaunt a number of security features including a unique identification number (including traceability code), password protection for read and write access, single or mutual authentication, and data transmission encryption.

New more security-conscious readers are expected to come to market within the next several months. They will support advanced, military-level 128-bit AES encryption, as well as simpler encryption algorithms. They will also allow password protection and optional encryption of multiple zones on the RFID tag.

Plan today for future changes

As they say, change is the only thing that is constant. This is true in the areas of security and RFID. Encryption algorithms are continually being updated and improved. Encryption keys only get longer and stronger. Finally, since RFID is a relatively new area, we can expect that the feature set on RFID tags will evolve over time to adjust to changing supply chain requirements.

Keep this in mind when selecting an RFID tag reader. Some readers can only be updated by manually changing the hardware inside the equipment. Imagine sending the facilities maintenance guy around to every entrance in a building to dismantle and update every card reader. Then imagine, sending an army of maintenance guys to every stop on the supply chain from the manufacturer to the consumer, to dismantle and update thousands of tag readers. Flexibility is key and help is on the way. New RFID readers will allow all the equipment in the network to be updated over the network, by simply uploading new firmware. By the end of this year, tag readers will be on the market that support Internet-based firmware upgrades. Such tag readers will allow multiple networks of readers to be updated from a single remote location.

Conclusion

RFID is taking off, with massive growth in the highly secure pharmaceutical, cashless transaction, and identity applications. These new applications require a lot more data, a lot more security, and the ability to securely accommodate multiple users. System integrators contemplating the use of RFID should begin by specifying a tag reader that supports the level of security required by the application and allows easy modification for future revisions and improvements. Tags should also be specified with sufficient memory to hold all the required data and with sufficient configurability to support all the different users in the chain, with individual zones. **EW**

Jean Pierre Benhammou is Atmel's RFID product marketing director. He holds a master's degree in physics from Marseille University and a doctorate in solid-state electronics from Montpellier University.

Martin Payne is SkyTek's vice president of marketing and strategy.